PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY
(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)* see form PCT/ISA/210 (second sheet)	
Applicant's or agent's file reference see form PCT/ISA/220	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/IB2004/050478	21.04.2004	22.04.2003

International Patent Classification (IPC) or both national classification and IPC
G06K19/073, G07F7/10, H04L9/06, G06F21/00

Applicant
KONINKLIJKE PHILIPS ELECTRONICS N.V.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☒ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☒ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA"). However, this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of three months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA:

European Patent Office
D-80298 Munich
Tel. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Authorized Officer

Heusler, N

Telephone No. +49 89 2399-2359

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of the international application in the language in which it was field, unless otherwise indicated under this item.

   ☐ This opinion has been established on the basis of a translation from the original language into the following language , which is the language of a translation furnished for the purposes of international search (under Rules 12.3 and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

   a. type of material:

   ☐ a sequence listing

   ☐ table(s) related to the sequence listing

   b. format of material:

   ☐ in written format

   ☐ in computer readable form

   c. time of filing/furnishing:

   ☐ contained in the international application as filed.

   ☐ filed together with the international application in computer readable form.

   ☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

Box No. II Priority

1. ☒ The following document has not been furnished:

   ☒ copy of the earlier application whose priority has been claimed (Rule 43*bis*.1 and 66.7(a)).

   ☐ translation of the earlier application whose priority has been claimed (Rule 43*bis*.1 and 66.7(b)).

   Consequently it has not been possible to consider the validity of the priority claim. This opinion has nevertheless been established on the assumption that the relevant date is the claimed priority date.

2. ☐ This opinion has been established as if no priority had been claimed due to the fact that the priority claim has been found invalid (Rules 43*bis*.1 and 64.1). Thus for the purposes of this opinion, the international filing date indicated above is considered to be the relevant date.

3. Additional observations, if necessary:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	2-6
	No:	Claims	1,7
Inventive step (IS)	Yes:	Claims	3,4
	No:	Claims	1,2,5-7
Industrial applicability (IA)	Yes:	Claims	1-7
	No:	Claims	

2. Citations and explanations

see separate sheet

Box No. VII Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

The following documents are cited:

D1: US 6,498,404 (corresponding to WO 00/26746 cited in the application)
D2: DE 198 28 936

Ad V.2 - novelty, inventive step; citations and explanations

1. The application **relates to** the protection of a chip card against differential power analysis: The power supply current consumed by the card may be used to identify secret information which is processed inside the card. The **problem** is to provide a flexible, effective means for cloaking of the effect of the secret information on the power supply current. The **solution** is to use an activity monitor, which evaluates pairs of processing signals that come into and out of processing circuits that process secret information. These measurements of the activity monitors are added and used to control the cloaking current that is drawn from the power supply so as to cloak the dependency on the secret information. The **gist** of the invention is that the excess current generated by the cloaking circuit depends on the processing actually done in the card.

2. However, it appears that the difference between the invention and the prior art is not yet fully expressed in the independent claims. As a consequence, also the known solution of D1 falls under **claim 1**.

   From D1 a chip card with obscured power consumption is known which uses a load circuit to draw an additional supply current in parallel with the secret information dependent supply current. A complementary circuit is used in addition to the circuitry that draws secrets information dependent power supply current. Both circuits contain similar circuit elements; in each clock cycle, complementary logic level changes are made in the complementary circuits so that the number of logic level changes in combination of both circuits does not change. Hence, the supply current does not depend on data which are actually processed.

   D1 discloses
   - an electronic device for executing operations dependent on secret information (D1, col. 1, from line 12), the device comprising
   - power supply connections (see D1, Fig. 1, and col. 2, from line 24)
   - a processing unit (see Fig. 2) with a plurality of processing circuits (such as AND-gate 5) for use in execution respective parts of the operations dependent on the secret information (obviously AND-gate 5 in D1 handles security relevant information), the processing circuit being fed from the power supply connections (this is implicitly disclosed in D1: the AND-gate 5 could not work without appropriate power supply)
   - an activity monitor circuit (inverters 6, 7 with AND-gate 8) coupled to receive pairs of processing signals (see Fig. 2: the monitoring circuit receives two signals) coming into (into gate 5) and out of (obviously, the two signals are output signals of any upstream

logic gates in Fig. 2) respective ones of the processing circuits, the monitor circuit being arranged to derive activity information (the logic signals being high or low) from each pair of processing signals, and to derive from the activity information a combined activity signal indicative of a sum of power supply currents that will be consumed by the processing circuits dependent on the processing signals (the two input signals are indicative of the current drawn by AND-gate 5),

- a current drawing circuit (AND-gate 8) connected to the power supply connections (again, implicitly disclosed: gate 8 could not work properly without power supply) and controlled by the activity monitor circuit to draw a cloaking current (additional AND-gate 8 serves to consume electrical current) controlled by the combined activity signal, so that power supply current variations dependent on the secret information are cloaked in combination of the cloaking current and the current drawn by the processing circuit (col. 3, lines 7-13).

As a consequence, the subject matter of **claim 1** lacks novelty (Art. 33 (2) PCT) over D1. A similar objection applies to **claim 7**. Any difference between the invention and D1 is not clearly defined in all independent claims.

3. The different components defined in **claims 2, 5 and 6** are obviously present in any electronic computer circuit. Even if this is not disclosed in D1, it is straightforward for a skilled person to include these modules in the circuit of D1. Therefore these claims add nothing inventive.

4. The pipelining arrangement defined in **claims 3 and 4** is not suggested by the prior art documents on hand.

5. D2 describes another possibility to protect a chip card or other electronic component against differential power analysis: capacitors are randomly connected to the supply voltage in order to cloak the supply current; this may only be done during encoding/decoding (col. 2, lines 15-18). Alternatively or in addition, the CPU may perform additional calculations based on random numbers which have no influence on the actual en-/decoding. Therefore the capacitors of D2 (Fig. 1) serve as a current drawing circuit as defined in claim 1 of the present application. D2 suggests to limit the cloaking to certain operating steps (col. 2, lines 15-18), which means that there has to be an activity monitor circuit which activates the capacitors and the random number generator as soon as the processor deals with security relevant data. Therefore this document discloses a security system very close to that of the application.

Certain defects (form and content, Rules 5 - 7 PCT)

4. The independent claims are not in the two-part-form (Rule 6.3b PCT).

5. D2 is not acknowledged in the description (Rule 5.1a PCT).